UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/411,070	10/04/1999	ROYCE E. SLICK	36J.P229	7819

5514 7590 03/31/2005

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
STULBERGER, CAS P	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 03/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/411,070	SLICK ET AL.	
	Examiner	Art Unit	
	Cas Stulberger	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-104 and 122-140* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-104 and 122-140* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. 02162005
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 10/04/1999; amendment filed 02/18/2005.

2. Claims 1-104, 122-140 are pending in the case. Claims are independent claims.

Response to Arguments

3. Applicant's arguments, see amendment, filed 02/18/2005, with respect to the rejection(s)of claim(s) 1-104, and 122-140 under 35 U.S.C 103(a) to Davis in view of Slavin have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of U.S. Patent No 6,385,728 B1 to DeBry.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-7, 11-14, 16, 17-22, 27-30, 32-38, 42-46, 48-54, 59-62, 64-70, 74-77, 79-85, 90-93, 95-101, 122-123, 125-131, and 136-139 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No 6,385,728 B1 to DeBry, and further in view of Non-Patent Literature Applied Cryptography Second Edition by Schneier.

6. In regards to claims 1, 16, 32, 48, 64, 79, 95, and 125, DeBry discloses the server encrypts the file with the printer's public key and sends the encrypted file to the printer. The printer then decrypts the encrypted file with the appropriate key (DeBry: column 10, lines 18-21). This meets the limitation of "encrypting the data using a first key, the first key being a public key of the first private key/public key pair being primarily in the sole possession of the intended image output device; and a transmitting step of transmitting the twice-encrypted data to the intended image output device." DeBry however does not disclose "twice encrypting the first key using a second key, the second key being a public key of a second private key/public key pair, the second key being primarily in the sole possession of the intended recipient of the image."

7. Schneier discloses double encryption (Schneier: Chapter 15, page 357). The same plaintext block is encrypted multiple times with multiple keys. Schneier also discloses to make sure the multiple keys are different and independent when using Multiple Key Encryption (Schneier: Chapter 15, Page 357). This meets the limitation of "twice encrypting the first key using a second key, the second key being a public key of a second private key/public key pair, the second key being primarily in the sole possession of the intended recipient of the image."

8. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of encrypting a file with the printer's public key as disclosed by DeBry with the method of using a different key to doubly encrypt the file as disclosed by Schneier in order to make the doubly-encrypted cipher text block harder to break using an exhaustive search (Schneier: Chapter 15, page 358).

9. In regards to claims 2, 6, 7, 13, 17, 20, 21, 29, 33, 37, 38, 45, 49, 52, 53, 61, 65, 69, 70, 76, 80, 83, 84, 92, 96, 100, 101, 122, 126, 129, 130, and 138, DeBry discloses the server sends the printer a print job encrypted with a symmetric key (DeBry: column 11, lines 2-4). When the printer receives the document it requests the key from the print server. The server sends the key, which is itself encrypted using the printer's public key. The printer decrypts the key and then uses the key to decrypt the document as it prints it (DeBry: column 11, lines 9-15). This meets the limitations of "a first encrypting step of encrypting the data using a first key; a second encrypting step of encrypting the first key using a second key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device; and a transmitting step of transmitting the encrypted data and the first key to the intended image output device." DeBry however does not disclose "twice encrypting the first key using a third key, the third key being a public key of a second private key/public key pair, the second key being primarily in the sole possession of the intended recipient of the image."

10. Schneier discloses double encryption (Schneier: Chapter 15, page 357). The same plaintext block is encrypted multiple times with multiple keys. Schneier also discloses to make sure the multiple keys are different and independent when using Multiple Key Encryption (Schneier: Chapter 15, Page 357). This meets the limitation of "twice encrypting the first key using a second key, the second key being a public key of a second private key/public key pair, the second key being primarily in the sole possession of the intended recipient of the image."

11. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of encrypting a file with the printer's public key as

disclosed by DeBry with the method of using a different key to doubly encrypt the file as disclosed by Schneier in order to make the doubly-encrypted cipher text block harder to break using an exhaustive search (Schneier: Chapter 15, page 358).

12. In regards to claims 3, 34, 66, and 97, DeBry does not disclose that the symmetric key is randomly generated.

13. Schneier discloses that good keys are random-bit stings generated by some automatic process (Schneier: Chapter 8.1, page 173).

14. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method using a symmetric key as disclosed by DeBry with the method of randomly generating the key as disclosed by Schneier in order to make the keys difficult to guess. (Schneier: Chapter 8.1, page 174)..

15. In regards to claims 4, 19, 35, 51, 67, 82, 98, and 128, DeBry discloses the server sends the printer a print job encrypted with a symmetric key (DeBry: column 11, lines 2-4).

16. In regards to claims 5, 18, 36, 50, 68, 81, 99, and 127, DeBry discloses the server sends the key, which is itself encrypted using the printer's public key (DeBry: column 11, lines 12-13).

17. In regards to claims 11, 27, 42, 59, 74, 90, and 136, DeBry discloses a printer (DeBry: column 12, lines 13-14.)

18. In regards to claims 12, 28, 43, 60, 75, 91, and 137, DeBry discloses a fax machine may be understood to be a printer in the context of this invention (DeBry: column 12, lines 20-22).

19. In regards to claims 14, 30, 46, 62, 77, 93, 123, and 139, DeBry discloses a transmitting device can be the Internet (DeBry: column 11, lines 41-42).

20. In regards to claims 22, 54, 85, and 131, this feature is inherent in any asymmetric key system. The private key is always securely stored so that only the key's owner has access to it. If anyone else had access to the private key in an asymmetric key system the security of the system would be compromised.

21. In regards to claim 44, DeBry disclose that client means any requester, and a printer, printer server, or printing system can be a fax machine (DeBry: column 12, lines 13-32). In the case of a fax system, it is known that one fax machine can request the transfer and printing of a file to another fax machine.

22. Claims 8, 9, 15, 23, 31, 39, 40, 47, 55, 63, 71, 72, 78, 86, 94, 102, 124, 132, and 140, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No 6,385,728 B1 to DeBry, in view of Non-Patent LiteratureApplied Cryptography Second Edition by Schneier, and in further view of U.S. Patent No 5,633,932 to Davis et al.

23. In regards to claims 23, 55, 86, and 132, DeBry does not disclose using a smart-card to store the second key which is possessed by the intended recipient.

24. Davis discloses using a smart-card at the printing node to authenticate the intended recipient. A standard challenge/response would occur between the printing node and the token to prove that the token is authentic and is in possession of the private key (Davis: Column 5, lines 33-35, 52-65).

25. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of encrypting a file with the user's public key as disclosed by DeBry with the method of using a smart-card to provided the private key to decrypt the file as disclosed by Davis in order to confirm the intended recipient at the printing node (Davis: column 5, lines 33-35).

26. In regards to claims 8, 9, 39, 40, 71, 72, and 102, DeBry does not disclose transmitting the key in the header.

27. Davis however discloses the header may contain a session key that is then used by both the sender and receiver to perform the required cryptographic operations on the document (Davis: column 4, lines 43-51). Information that is related to the identity of a device or person initiating the transmission would be the IP address of the header.

28. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of doubly encrypting a symmetric key as disclosed by DeBry with the method of putting the key in the header as disclosed by Davis in order to reduce the computational performance normally associated with public key cryptography (Davis: column 4, lines 51-54).

29. In regards to claims 15, 31, 47, 63, 78, 94, 124, and 140, Debry does not disclose the header containing a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

30. Davis discloses the header contains includes control information (Davis: column 4, lines 56-67).

31. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of encryption as disclosed by DeBry with the method of putting control information in the header as disclosed by Davis in order to reduce the computational performance (Davis: column 4, lines 51-54).

32. Claims 10, 24-26, 41, 56-58, 73, 87-89, 103-104, 133-135, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No 6,385,728 B1 to DeBry, in view of Non-Patent LiteratureApplied Cryptography Second Edition by Schneier, and in further view of U.S. Patent No 6,226,618 B1 to Downes et al.

33. In regards to claims 10, 24-26, 41, 56-58, 73, 87-89, 103-104, 133-135, DeBry does not disclose hashing the headers and the data and signing it with a private key.

34. Downes discloses hashing the data and the symmetric key and encrypting to produce a digest. Then the digest is signed to create a digital signature (Downes: column 15, lines 53-67; column 16, lines 1-20). When the receiver receives the digest, it computes its own digest and compares the two. If the are not the same the digest is discarded and the sender is notified (Downes: column 16, step 412).

35. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method secure transmission as disclosed by DeBry with the method of creating a digest and verifying as disclosed by Downes in order to protect the integrity of the message (Downes: column 13, lines 49-51).

Conclusion

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cas Stulberger whose telephone number is (571) 272-3810. The examiner can normally be reached on Monday - Friday, 9:00A.M. - 6:00P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3810. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CS

CS

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100